On polarised class groups of orders in quartic CM-fields

Gaetan Bisson* Marco Streng†

February 18, 2013

Abstract

We give an explicit characterisation of pairs of orders in a quartic CM-field that admit the same polarised ideal class group structure. This generalises a simpler result for imaginary quadratic fields. We give applications to computing endomorphism rings of abelian surfaces over finite fields, and extending a completeness result of Murabayashi and Umegaki [10] to a list of abelian surfaces over the rationals with complex multiplication by arbitrary orders.

1 Introduction

Let $\mathcal{A}$ be a principally polarised abelian surface defined over a characteristic-zero field k, and assume that $\mathcal{A}$ has *complex multiplication (CM)*, by which we mean that the endomorphism algebra $K = \mathbb{Q} \otimes \mathrm{End}(\mathcal{A}_{\overline{k}})$ is a field of degree 4. This excludes abelian varieties that are not simple over the algebraic closure, and it implies that K is a quartic CM-field, that is, a totally imaginary quadratic extension of a real quadratic field K_0. The endomorphism ring $\mathcal{O} = \mathrm{End}(\mathcal{A}_{\overline{k}})$ of $\mathcal{A}$ is an order in K that is stable under complex conjugation. We will study the following group $\mathfrak{C}(\mathcal{O})$, for which the set of isomorphism classes of principally polarised abelian surfaces with endomorphism ring $\mathcal{O}$ of any given *CM-type* is a principal homogeneous space if it is non-empty, with group elements acting as isogenies. It was introduced by Shimura and Taniyama [12, §14] in the case $\mathcal{O} = \mathcal{O}_K$.

Definition 1. *Let $I_{\mathcal{O}}$ be the group of pairs $(\mathfrak{a}, \alpha)$ where $\mathfrak{a}$ is an invertible fractional ideal of $\mathcal{O}$ satisfying $\mathfrak{a}\overline{\mathfrak{a}} = \alpha\mathcal{O}$ for some totally positive element α of K_0, endowed with component-wise multiplication, and let $P_{\mathcal{O}}$ be the subgroup formed by pairs of the form $(x\mathcal{O}, x\overline{x})$ for $x \in K^\times$. The quotient $I_{\mathcal{O}}/P_{\mathcal{O}}$ is called the* polarised ideal class group *of $\mathcal{O}$ and is written $\mathfrak{C}(\mathcal{O})$.*

In what follows, we restrict $\mathfrak{a}$ and $x\mathcal{O}$ in the definitions of $I_{\mathcal{O}}$ and $P_{\mathcal{O}}$ to be coprime to a fixed integer f. This has no effect on the group $\mathfrak{C}(\mathcal{O})$, but it allows us to compare the groups more effectively as the order $\mathcal{O}$ varies.

*Macquarie University, Sydney, Australia. http://www.normalesup.org/~bisson/

†VU University Amsterdam, The Netherlands. Supported by EPSRC grant number EP/G004870/1 and by the Netherlands Organisation for Scientific Research (NWO) through the DIAMANT research cluster. http://www.few.vu.nl/~streng/

This group and more specifically its subgroup generated by the reflex type norm (Section 2) is significant to a number of problems. For instance, the faithfulness and transitivity of its action as isogenies has been exploited to compute endomorphism rings of abelian surfaces [2], which requires in particular to tell orders $\mathcal{O}$ apart using the structure of their groups $\mathfrak{C}(\mathcal{O})$; here, we establish in how far this is possible.

As a second application, we use these groups to extend a completeness result of Murabayashi and Umegaki [10] which allows us to prove that van Wamelen's conjectural list of principally polarised abelian surfaces with complex multiplication over the rationals [19] is in fact correct, as well as to conjecture its generalization to non-maximal orders (Section 6.1).

2 Statement of the results

For any two orders $\mathcal{O} \subset \mathcal{O}'$, invertible ideals of $\mathcal{O}$ coprime to the index $f = [\mathcal{O}_K : \mathcal{O}]$ are in natural bijection with those of $\mathcal{O}'$ via the map $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}'$. This extends trivially to injections $I_{\mathcal{O}} \to I_{\mathcal{O}'}$ and $P_{\mathcal{O}} \to P_{\mathcal{O}'}$ (where we restrict as in Section 1 to ideals coprime to f), which yield a natural morphism $\mathfrak{C}(\mathcal{O}) \to \mathfrak{C}(\mathcal{O}')$. We will use these maps implicitly and say for instance that an ideal $\mathfrak{a}$ is principal in $\mathcal{O}'$ when we actually mean that $\mathfrak{a}\mathcal{O}'$ is.

Let K be a CM-field. A CM-type Φ of K with values in $\mathbb{C}$ is a complete set of representatives for the embeddings $K \to \mathbb{C}$ up to complex conjugation. The *reflex field* $K^r \subset \mathbb{C}$ of Φ is the subfield generated by the image of the *type norm*

$$\mathrm{N}_\Phi : x \in K \mapsto \prod_{\phi \in \Phi} \phi(x) \in \mathbb{C}.$$

The *reflex type* [12, §8] is the set $\Phi^r = \{\psi^{-1}_{|K^r} : \psi \in S\}$ of embeddings of K^r into the normal closure K^c of K, where S is the set of all embeddings of K^c into $\mathbb{C}$ that extend elements of Φ. It is a CM-type of K^r with values in K^c and reflex field K, hence defines a type norm $\mathrm{N}_{\Phi^r} : K^r \to K$. This norm can be extended into a homomorphism from the group $I_{K^r} = I_{K^r}(f)$ of invertible ideals $\mathfrak{a}$ of $\mathcal{O}_{K^r}$ coprime to f to the analogous group for $\mathcal{O}$. In turn, this defines a map

$$\begin{aligned} I_{K^r}(f) &\longrightarrow \mathfrak{C}(\mathcal{O}), \\ \mathfrak{a} &\longmapsto (\mathrm{N}_{\Phi^r}(\mathfrak{a}), \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{a})). \end{aligned} \tag{1}$$

We denote its kernel by $S_{\mathcal{O}}$. It is an important object, because the image $I_{K^r}(f)/S_{\mathcal{O}}$ appears naturally as the Galois group of the field of moduli of the abelian surfaces of type Φ with endomorphism ring $\mathcal{O}$ [12, Main Theorem 3 on page 142]. Our main results are the following two theorems, and their applications in Section 6 as mentioned in the introduction.

Theorem 2. *If $S_{\mathcal{O}_K} \subset S_{\mathcal{O}}$, then all prime factors of the index $[\mathcal{O}_K : \mathcal{O}]$ divide $2 \cdot 3 \cdot N_{K_0/\mathbb{Q}}(\mathrm{disc}(K/K_0))$.*

For a pair of general orders $\mathcal{O}, \mathcal{O}' \subset K$, let $\mathcal{O}^\circ$ be their intersection, and use a subscript 0 to denote intersections with K_0, which are orders in K_0.

Theorem 3. *If $S_{\mathcal{O}} \subset S_{\mathcal{O}'}$ and $\mathcal{O} \ncong \mathbb{Z}[\zeta_5]$, then the quotient $[\mathcal{O} : \mathcal{O}^\circ]/[\mathcal{O}_0 : \mathcal{O}_0^\circ]$ is an integer, and is not divisible by any prime $p > 3$.*

3 From ideals to elements

If $\mathcal{O}$ and $\mathcal{O}'$ are two orders of a quartic CM-field K, we obviously have the implication $\mathcal{O} \subset \mathcal{O}' \Rightarrow S_{\mathcal{O}} \subset S_{\mathcal{O}'}$. The goal of Section 4 is to establish a partial converse to this statement, that is, to obtain an explicit condition on $\mathcal{O}$ and $\mathcal{O}'$ necessary for $S_{\mathcal{O}} \subset S_{\mathcal{O}'}$ to hold. To help us with that, we first express some relevant groups in terms of ring *elements*, as opposed to ideals.

We denote by $\mathcal{O}^\circ$ the intersection of $\mathcal{O}$ and $\mathcal{O}'$. The corresponding orders in the totally real subfield K_0 will be written $\mathcal{O}_0 = \mathcal{O} \cap K_0$ and $\mathcal{O}_0^\circ = \mathcal{O}^\circ \cap K_0$. Finally, we fix $f = [\mathcal{O}_K : \mathcal{O}^\circ]$ once and for all.

Lemma 4. *All squares of $\mathfrak{C}(\mathcal{O}^\circ)$ are in the image of* (1).

Proof. Let σ be the non-trivial automorphism of K_0. Given any $(\mathfrak{a}, \alpha) \in I_{\mathcal{O}^\circ}$, we have

$$(\mathfrak{a}, \alpha)^2 = (\alpha^\sigma \mathcal{O}^\circ, (\alpha^\sigma)^2)^{-1} (\mathfrak{a}^2 (\mathfrak{a}\overline{\mathfrak{a}})^\sigma, N_{K_0/\mathbb{Q}}(\alpha)^2). \tag{2}$$

The first factor is trivial in $\mathfrak{C}(\mathcal{O}^\circ)$, and we claim that the second is the reflex type norm of $N_\Phi(\mathfrak{a})$. Indeed, we have first of all $N_{\Phi^r}(N_\Phi(\mathfrak{a})) = \mathfrak{a}^2(\mathfrak{a}\overline{\mathfrak{a}})^\sigma$, which is shown in the proof of [16, Lemma 2.6], and stated for maximal orders (but the proof is correct in general) in [15, Lemma I.8.4]. We also have $N_{K^r/\mathbb{Q}}(N_\Phi(\mathfrak{a})) = N_{K/\mathbb{Q}}(\mathfrak{a})^2 = N_{K_0/\mathbb{Q}}(\alpha)^2$, as K and K^r have equal degree and Φ contains two embeddings. This proves that the class of $(\mathfrak{a}, \alpha)^2$ is in the image. □

By Lemma 4, a necessary condition for $S_{\mathcal{O}} \subset S_{\mathcal{O}'}$ is

$$\ker(\mathfrak{C}(\mathcal{O}^\circ)^2 \to \mathfrak{C}(\mathcal{O})) \quad \subset \quad \ker(\mathfrak{C}(\mathcal{O}^\circ)^2 \to \mathfrak{C}(\mathcal{O}')), \tag{3}$$

and, to write these kernels in terms of ring elements, we use the following lemma.

Lemma 5. *Denote by ϕ the natural morphism $\mathfrak{C}(\mathcal{O}^\circ) \to \mathfrak{C}(\mathcal{O})$ and consider the relative norm*

$$\psi : \frac{(\mathcal{O}/f\mathcal{O}_K)^\times}{(\mathcal{O}^\circ/f\mathcal{O}_K)^\times \mu_{\mathcal{O}}} \longrightarrow \frac{(\mathcal{O}_0/f\mathcal{O}_{K_0})^\times}{(\mathcal{O}_0^\circ/f\mathcal{O}_{K_0})^\times}. \tag{4}$$

We have $\ker\phi = \ker\psi$ *and* $\operatorname{coker}\phi \subset \operatorname{coker}\psi$.

Proof. The diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & P_{\mathcal{O}^\circ} & \longrightarrow & I_{\mathcal{O}^\circ} & \longrightarrow & \mathfrak{C}(\mathcal{O}^\circ) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \phi} & & \\
1 & \longrightarrow & P_{\mathcal{O}} & \longrightarrow & I_{\mathcal{O}} & \longrightarrow & \mathfrak{C}(\mathcal{O}) & \longrightarrow & 1
\end{array}$$

has exact rows and, as we restrict to ideals coprime to f, its two leftmost vertical arrows are injective. The snake lemma thus tells us that

$$(\text{co})\ker\phi = (\text{co})\ker\left(\frac{P_{\mathcal{O}}}{P_{\mathcal{O}^\circ}} \to \frac{I_{\mathcal{O}}}{I_{\mathcal{O}^\circ}}\right).$$

It now suffices to give a natural isomorphism and an embedding

$$\frac{P_{\mathcal{O}}}{P_{\mathcal{O}^\circ}} = \frac{(\mathcal{O}/f\mathcal{O}_K)^\times}{(\mathcal{O}^\circ/f\mathcal{O}_K)^\times \mu_{\mathcal{O}}}, \qquad \frac{I_{\mathcal{O}}}{I_{\mathcal{O}^\circ}} \hookrightarrow \frac{(\mathcal{O}_0/f\mathcal{O}_{K_0})^\times}{(\mathcal{O}_0^\circ/f\mathcal{O}_{K_0})^\times}$$

such that the induced map is ψ. For these maps, we obviously take $(x\mathcal{O}, x\overline{x}) \mapsto x$ (for integral representatives $(x\mathcal{O}, x\overline{x})$ of elements of $P_{\mathcal{O}}/P_{\mathcal{O}^\circ}$) and $(\mathfrak{a}, \alpha) \mapsto \alpha$ (for integral representatives $(\mathfrak{a}, \alpha)$ of elements of $I_{\mathcal{O}}/I_{\mathcal{O}^\circ}$).

On $P_{\mathcal{O}}$, the first map is well-defined, as $(x\mathcal{O}, x\overline{x})$ determines x up to roots of unity in $\mathcal{O}$. The kernel then consists of those pairs $(x\mathcal{O}, x\overline{x})$ with x in $\mathcal{O}^\circ$ invertible modulo f, that is, such that $x\mathcal{O}^\circ$ is coprime to f. In other words, the kernel is $P_{\mathcal{O}^\circ}$, so the map is indeed well-defined and injective on $P_{\mathcal{O}}/P_{\mathcal{O}^\circ}$. Surjectivity is obvious.

The second map is well-defined on $I_{\mathcal{O}}/I_{\mathcal{O}^\circ}$. Now suppose that $(\mathfrak{a}, \alpha)$ is in the kernel, again without loss of generality with $\mathfrak{a}$ integral. Then $\alpha\mathcal{O}_0^\circ$ is coprime to f, so $\alpha\mathcal{O}^\circ$ is also coprime to f. Denoting by $\mathfrak{b}$ the unique $\mathcal{O}^\circ$-ideal coprime to f satisfying $\mathfrak{a} = \mathfrak{b}\mathcal{O}$, we have $\mathfrak{b}\overline{\mathfrak{b}}\mathcal{O} = \alpha\mathcal{O}$ and, as $\alpha\mathcal{O}^\circ$ and $\mathfrak{b}$ are coprime to f, we find $(\mathfrak{b}, \alpha) \in I_{\mathcal{O}^\circ}$ which implies $(\mathfrak{a}, \alpha) \in I_{\mathcal{O}^\circ}$ by abuse of notation. This proves injectivity.

Finally, the induced map ψ is indeed the relative norm, as x maps via $(x\mathcal{O}, x\overline{x})$ to $x\overline{x}$. □

Using Lemma 5, the necessary condition (3) becomes as follows.

Proposition 6. *If two orders $\mathcal{O}$ and $\mathcal{O}'$ of a quartic CM-field satisfy $S_{\mathcal{O}} \subset S_{\mathcal{O}'}$, then the kernel*

$$\ker\left(\psi : \frac{(\mathcal{O}/f\mathcal{O}_K)^\times}{(\mathcal{O}^\circ/f\mathcal{O}_K)^\times \mu_{\mathcal{O}}} \to \frac{(\mathcal{O}_0/f\mathcal{O}_{K_0})^\times}{(\mathcal{O}_0^\circ/f\mathcal{O}_{K_0})^\times}\right) \tag{5}$$

is of exponent at most two.

Proof. By (3), if $S_{\mathcal{O}} \subset S_{\mathcal{O}'}$, then we have

$$\begin{aligned}\ker\left(\mathfrak{C}(\mathcal{O}^\circ) \to \mathfrak{C}(\mathcal{O})\right)^2 &\subset \ker\left(\mathfrak{C}(\mathcal{O}^\circ)^2 \to \mathfrak{C}(\mathcal{O})\right)\\ &\subset \ker\left(\mathfrak{C}(\mathcal{O}^\circ)^2 \to \mathfrak{C}(\mathcal{O}')\right) \subset \ker\left(\mathfrak{C}(\mathcal{O}^\circ) \to \mathfrak{C}(\mathcal{O}')\right),\end{aligned}$$

hence

$$\ker\left(\mathfrak{C}(\mathcal{O}^\circ) \to \mathfrak{C}(\mathcal{O})\right)^2 \quad \subset \quad \ker\left(\mathfrak{C}(\mathcal{O}^\circ) \to \mathfrak{C}(\mathcal{O}')\right) \cap \ker\left(\mathfrak{C}(\mathcal{O}^\circ) \to \mathfrak{C}(\mathcal{O})\right).$$

Applying Lemma 5 to both $\mathcal{O}$ and $\mathcal{O}'$, and noting $(\mathcal{O}'/f\mathcal{O}_K)^\times \cap (\mathcal{O}/f\mathcal{O}_K)^\times = (\mathcal{O}^\circ/f\mathcal{O}_K)^\times$, this becomes

$$\begin{aligned}&\ker\left(\frac{(\mathcal{O}/f\mathcal{O}_K)^\times}{(\mathcal{O}^\circ/f\mathcal{O}_K)^\times}/\mu_{\mathcal{O}} \to \frac{(\mathcal{O}_0/f\mathcal{O}_{K_0})^\times}{(\mathcal{O}_0^\circ/f\mathcal{O}_{K_0})^\times}\right)^2\\ \subset &\ker\left(\frac{(\mathcal{O}^\circ/f\mathcal{O}_K)^\times}{(\mathcal{O}^\circ/f\mathcal{O}_K)^\times}/\mu_{\mathcal{O}^\circ} \to \frac{(\mathcal{O}_{K_0}/f\mathcal{O}_{K_0})^\times}{(\mathcal{O}_0^\circ/f\mathcal{O}_{K_0})^\times}\right) = 1.\end{aligned}$$ □

Note that, unless $\mathcal{O} \cong \mathbb{Z}[\zeta_5]$, the unit group $\mu_{\mathcal{O}} = \{\pm 1\}$ can be absorbed into $(\mathcal{O}^\circ/f\mathcal{O}_K)^\times$.

4 Explicit bounds

We shall now derive from Proposition 6 a more explicit necessary condition for $S_{\mathcal{O}} \subset S_{\mathcal{O}'}$ on the indices of the relevant orders. First, let us give a weak but natural result bounding the size of the quotient groups of Equation (5) in terms of these indices.

Proposition 7. *Let $\mathcal{O}^\circ \subset \mathcal{O}$ be two orders in a number field K of degree n, and let f be a multiple of the index $[\mathcal{O} : \mathcal{O}^\circ]$; we have*

$$[\mathcal{O} : \mathcal{O}^\circ] \prod_{p|f} (1 - 1/p)^n \leq \left| \frac{(\mathcal{O}/f\mathcal{O})^\times}{(\mathcal{O}^\circ/f\mathcal{O})^\times} \right| \leq [\mathcal{O} : \mathcal{O}^\circ].$$

Proof. Decomposing the ring $\mathcal{O}/f\mathcal{O}$ over prime ideals $\mathfrak{p}$ of $\mathcal{O}$ dividing f yields

$$\left|(\mathcal{O}/f\mathcal{O})^\times\right| = |(\mathcal{O}/f\mathcal{O})| \prod_{\mathfrak{p}} (1 - 1/\operatorname{N}(\mathfrak{p})).$$

Since there are at most n such $\mathfrak{p}$ dividing each prime factor p of f, we derive

$$\frac{|(\mathcal{O}/f\mathcal{O})^\times|}{|(\mathcal{O}^\circ/f\mathcal{O})^\times|} \geq \frac{|(\mathcal{O}/f\mathcal{O})|}{|(\mathcal{O}^\circ/f\mathcal{O})|} \prod_{\mathfrak{p}} (1 - 1/\operatorname{N}(\mathfrak{p})) = [\mathcal{O} : \mathcal{O}^\circ] \prod_{p|f} (1 - 1/p)^n. \qquad \square$$

Asymptotically as the index $[\mathcal{O} : \mathcal{O}^\circ]$ goes to infinity, the quotient group grows as fast as the index, with an error factor $O(\log\log([\mathcal{O} : \mathcal{O}^\circ])^n)$. This natural result bounds the order of the kernel (5) from below in terms of the quantity $[\mathcal{O} : \mathcal{O}^\circ]/[\mathcal{O}_0 : \mathcal{O}_0^\circ]$. We can study this bound one prime $p \mid f$ at a time, and note that the number of generators of $(\mathcal{O}/f\mathcal{O}_K)^\times$ is bounded as well, thus giving a lower bound on the exponent of the group (5). However we get a sharper criterion for having exponent greater than 2, if we disregard Proposition 7 and look more closely at the structure of the groups.

Proposition 8. *If the kernel* (5) *contains no element of order greater than two, then for every prime p we have $\operatorname{val}_p([\mathcal{O} : \mathcal{O}^\circ]) = \operatorname{val}_p([\mathcal{O}_0 : \mathcal{O}_0^\circ])$, except possibly for $p \leq 3$, and except possibly for $p \leq 19$ if $\mathcal{O} = \mathbb{Z}[\zeta_5]$.*

Proof. Assume that the kernel (5) is of exponent one or two, and suppose that there exists a prime $p \geq 5$ at which the quotient $[\mathcal{O} : \mathcal{O}^\circ]/[\mathcal{O}_0 : \mathcal{O}_0^\circ]$ is nontrivial.

To better work with this kernel, we first write the domain and codomain of the relative norm map of (5) more explicitly by decomposing the p-part of the ring $\mathcal{O}/f\mathcal{O}_K$ over primes ideals $\mathfrak{q}$ of $\mathcal{O}$ dividing $(p) = p\mathcal{O}$; this gives

$$(\mathcal{O}/(f\mathcal{O}_K)_{(p)})^\times = \prod_{\mathfrak{q}} (\mathcal{O}/(f\mathcal{O}_K)_{(\mathfrak{q})})^\times \cong \prod_{\mathfrak{q}} (\mathcal{O}/\mathfrak{q})^\times \times \frac{1 + \mathfrak{q}}{1 + (f\mathcal{O}_K)_{(\mathfrak{q})}},$$

where $I_{(\mathfrak{q})}$ denotes the $\mathfrak{q}$-primary part of I, i.e., $I_{(\mathfrak{q})} = (I \cdot \mathcal{O}_\mathfrak{q}) \cap \mathcal{O} = I + \mathfrak{q}^n$ for all sufficiently large n (see [14]). Therefore, omitting the case $\mathcal{O} \cong \mathbb{Z}[\zeta_5]$ for now, we can assume that quotienting out by $\mu_\mathcal{O} = \{\pm 1\}$ is trivial and the domain from (5) can be written locally at p as

$$D := \frac{(\mathcal{O}/(f\mathcal{O}_K)_{(p)})^\times}{(\mathcal{O}^\circ/(f\mathcal{O}_K)_{(p)})^\times} \cong \frac{\prod_\mathfrak{q} (\mathcal{O}/\mathfrak{q})^\times}{\prod_\mathfrak{p} (\mathcal{O}^\circ/\mathfrak{p})^\times} \times A_p;$$

for some p-group A_p. Similarly, the codomain can be written locally at p as

$$C := \frac{(\mathcal{O}_0/(f\mathcal{O}_{K_0})_{(p)})^\times}{(\mathcal{O}_0^\circ/(f\mathcal{O}_{K_0})_{(p)})^\times} \cong \frac{\prod_{\mathfrak{q}_0} (\mathcal{O}_0/\mathfrak{q}_0)^\times}{\prod_{\mathfrak{p}_0} (\mathcal{O}_0^\circ/\mathfrak{p}_0)^\times} \times A_{0,p}.$$

The rightmost factors $A_{0,p} \subset A_p$ are p-groups and, as p is odd and the kernel (5) has exponent at most two, they are equal.

Since $\mathcal{O}_0$ and $\mathcal{O}_0^\circ$ are quadratic, the non-p-part of the codomain C is cyclic and of order 1, $p-1$, or $p+1$. Correspondingly, the p-part $[\mathcal{O}_0 : \mathcal{O}_0^\circ]_p$ of the index is $\#A_{0,p}$ in the first case and $p \cdot \#A_{0,p}$ in the other cases.

On the other hand, the domain D is a product of cyclic groups with orders of the form p^e, $p^f - 1$, and $(p^g - 1)/(p^h - 1)$ where the exponents f, g, h, are in $\{1, 2, 4\}$ and $h < g$. The valuation at p of the index $[\mathcal{O} : \mathcal{O}^\circ]$ is then the sum of all e's, f's, and $(g-h)$'s. As the exponent of the kernel is at most two, the order of each of the coprime-to-p cyclic factors must divide the non-p-part of $2\#C$, which is 2, $2(p-1)$, or $2(p+1)$.

As $p \geq 5$, it is easy to see that $p^f - 1$ and $(p^g - 1)/(p^h - 1)$ do not divide $2\#C$, except when they are equal to $\#C/\#A_{0,p} \in \{p-1, p+1\}$. As these numbers are greater than three, this observation also shows that if there were multiple such cyclic factors in D, it would contradict the fact that a quotient by a 2-torsion subgroup is contained in C.

In particular, we get $\mathrm{val}_p([\mathcal{O} : \mathcal{O}^\circ]) \in \{\#A_p, \#A_p + 1\}$, where the second is possible only when $[\mathcal{O}_0 : \mathcal{O}_0^\circ] = \#A_{0,p} + 1$. We conclude $\mathrm{val}_p([\mathcal{O} : \mathcal{O}^\circ]) = \mathrm{val}_p([\mathcal{O}_0 : \mathcal{O}_0^\circ])$.

It remains to consider the case $\mathcal{O} \cong \mathbb{Z}[\zeta_5]$ where $\mu_\mathcal{O} \simeq \mathbb{Z}/10\mathbb{Z}$. In this case, the orders of the cyclic factors of D must divide $10\#C$, and the proof goes through for $p > 19$. □

Theorem 3. *If $S_\mathcal{O} \subset S_{\mathcal{O}'}$ and $\mathcal{O} \ncong \mathbb{Z}[\zeta_5]$, then the quotient $[\mathcal{O} : \mathcal{O}^\circ]/[\mathcal{O}_0 : \mathcal{O}_0^\circ]$ is an integer, and is not divisible by any prime $p > 3$.*

Proof. This is a combination of Propositions 6 and 8. □

5 A stronger result in the maximal case

The result of Proposition 8, namely that $\mathrm{val}_p[\mathcal{O} : \mathcal{O}^\circ] = \mathrm{val}_p[\mathcal{O}_0 : \mathcal{O}_0^\circ]$ for all but finitely many primes p, may not seem very strong. Only when $\mathcal{O}_0 = \mathcal{O}_0^\circ$ does it immediately imply that $\mathcal{O}$ and $\mathcal{O}^\circ$ are identical locally at all $p > 3$. The goal of this section is to prove that, in the case $\mathcal{O}' = \mathcal{O}_K$, Proposition 8 further implies that $\mathcal{O}_K$ and $\mathcal{O}$ are identical locally if we rule out a few more primes p.

Theorem 2. *If $S_{\mathcal{O}_K} \subset S_\mathcal{O}$, then all prime factors of the index $[\mathcal{O}_K : \mathcal{O}]$ divide $2 \cdot 3 \cdot N_{K_0/\mathbb{Q}}(\mathrm{disc}(K/K_0))$.*

To prove the theorem, we first give a result showing that $[\mathcal{O}_{K_0} : \mathcal{O}_0]$ almost divides the quotient $[\mathcal{O}_K : \mathcal{O}]/[\mathcal{O}_{K_0} : \mathcal{O}_0]$.

Lemma 9. *Let $K_0/\mathbb{Q}$ be a quadratic field and K/K_0 a finite Galois extension of degree n. Let $\mathcal{O}$ be an order of K stable under $\mathrm{Gal}(K/K_0)$, and let $\mathcal{O}_0 = \mathcal{O} \cap K_0$. Then we have*

$$[\mathcal{O}_{K_0} : \mathcal{O}_0]^{2n} \;\mid\; N_{K_0/\mathbb{Q}}(\mathrm{disc}(K/K_0))\ [\mathcal{O}_K : \mathcal{O}]^2. \tag{6}$$

Proof. Write $\mathcal{O}_{K_0} = \mathbb{Z} + \omega\mathbb{Z}$, $\mathcal{O}_0 = \mathbb{Z} + c\omega\mathbb{Z}$, $\delta = 2\omega - \mathrm{tr}_{K_0/\mathbb{Q}}(\omega)$, where $c \in \mathbb{Z}$. Note that (δ) is the different of K_0 and that $c = [\mathcal{O}_{K_0} : \mathcal{O}_0]$.

First of all, we have $\mathrm{tr}_{K/\mathbb{Q}}(\mathcal{O}/\delta) = \mathrm{tr}_{K_0/\mathbb{Q}}(\mathrm{tr}_{K/K_0}(\mathcal{O})/\delta)$. Using the fact that K/K_0 is Galois and $\mathcal{O}$ is stable under Galois, we find $\mathrm{tr}_{K/K_0}(\mathcal{O}) \subset \mathcal{O}_0$, so $\mathrm{tr}_{K/\mathbb{Q}}(\mathcal{O}/\delta) \subset \mathrm{tr}_{K_0/\mathbb{Q}}(\mathcal{O}_0/\delta) = c\mathbb{Z}$. In particular, $\mathcal{O}/(c\delta)$ is contained in the trace dual $\mathcal{O}^*$ of $\mathcal{O}$, so the following index is an integer:

$$\begin{aligned}[\mathcal{O}^* : \mathcal{O}/(c\delta)] &= N_{K/\mathbb{Q}}(c\delta)^{-1}[\mathcal{O}^* : {\mathcal{O}_K}^*][{\mathcal{O}_K}^* : \mathcal{O}_K][\mathcal{O}_K : \mathcal{O}] \\ &= c^{-2n}(\mathrm{disc}(K_0/\mathbb{Q}))^{-n}[\mathcal{O}^* : {\mathcal{O}_K}^*](\mathrm{disc}(K/\mathbb{Q}))[\mathcal{O}_K : \mathcal{O}] \\ &= c^{-2n}N_{K_0/\mathbb{Q}}(\mathrm{disc}(K/K_0))[\mathcal{O}^* : {\mathcal{O}_K}^*][\mathcal{O}_K : \mathcal{O}].\end{aligned}$$

Linear algebra gives us $[\mathcal{O}^* : {\mathcal{O}_K}^*] = [\mathcal{O}_K : \mathcal{O}]$, and the result follows. □

Corollary 10. *In the situation of Lemma 9, assume $n = 2$. If p divides $[\mathcal{O}_K : \mathcal{O}]$, but not $N_{K_0/\mathbb{Q}}(\mathrm{disc}(K/K_0))$, then p divides $[\mathcal{O}_K : \mathcal{O}]/[\mathcal{O}_{K_0} : \mathcal{O}_0]$.*

Proof. If p does not divide $[\mathcal{O}_{K_0} : \mathcal{O}_0]$, then the result is trivial. If p does divide that index, then Lemma 9 shows that p also divides the quotient $[\mathcal{O}_K : \mathcal{O}]/[\mathcal{O}_{K_0} : \mathcal{O}_0]$. □

Proof of Theorem 2. For $K \ncong \mathbb{Q}(\zeta_5)$, the theorem follows immediately from Corollary 10 and Proposition 8.

For $K = \mathbb{Q}(\zeta_5)$, these results still leave the primes $7 \leq p \leq 19$ open, with which we deal by explicit computation. Indeed, if $p|[\mathcal{O}_K : \mathcal{O}]$ and $S_{\mathcal{O}_K} \subset S_{\mathcal{O}}$, then the same holds with $\mathcal{O}$ replaced by $\mathcal{O}+p\mathcal{O}_K$, for which there are only finitely many possibilities, which are easily enumerated by a computer program. □

Example 11. The factor $N_{K_0/\mathbb{Q}}(\mathrm{disc}(K/K_0))$ on the right hand side of (6) cannot be omitted. Consider for instance the order

$$\mathcal{O} = \mathbb{Z}[z^2, \frac{1}{34}(17 + 172z + 24z^2 + z^3)]$$

where z satisfies $z^4 + 7z^3 + 36z^2 + 119z + 289 = 0$; both $\mathcal{O}$ and $\mathcal{O}_0 = \mathbb{Z}[7(z + \overline{z})]$ have index 7 in their respective maximal orders, so Lemma 9 would be false without that factor. Moreover, we have $S_{\mathcal{O}} = S_{\mathcal{O}_K}$, showing that the discriminant factor is also necessary in Theorem 2.

6 Applications

6.1 Abelian surfaces with complex multiplication over the rationals

6.1.1 Statements

Van Wamelen [18] gives a conjectural list of curves of genus two defined over $\mathbb{Q}$ with complex multiplication by maximal orders. Our results allow us to finish the proof of this list, as well as to conjecture its generalisation to arbitrary orders.

Theorem 12. *The 19 curves given in [18] are (up to $\overline{\mathbb{Q}}$-isomorphism) exactly the curves $C/\mathbb{Q}$ of genus two with $\mathrm{End}(J(C)_{\overline{\mathbb{Q}}}) \cong \mathcal{O}_K$ for a quartic CM-field K.*

Theorem 13. *The curve*

$$C : y^2 = x^6 - 4x^5 + 10x^3 - 6x - 1$$

has endomorphism ring

$$\mathrm{End}(J(C)_{\overline{\mathbb{Q}}}) \cong \mathbb{Z} + 2\zeta_5\mathbb{Z} + (\zeta_5^2 + \zeta_5^3)\mathbb{Z} + 2\zeta_5^3\mathbb{Z},$$

and there exists a curve $D/\overline{\mathbb{Q}}$ of genus two with endomorphism ring

$$\mathrm{End}(J(D)_{\overline{\mathbb{Q}}}) \cong \mathbb{Z} + (\zeta_5 + 3\zeta_5^3)\mathbb{Z} + (\zeta_5^2 + \zeta_5^3)\mathbb{Z} + 5\zeta_5^3\mathbb{Z}$$

and absolute Igusa invariants in $\mathbb{Q}$. Moreover, the curves C and D are (up to $\overline{\mathbb{Q}}$-isomorphism) the only curves of genus two with field of moduli $\mathbb{Q}$ such that $\mathrm{End}(J(C)_{\overline{\mathbb{Q}}})$ *is a* non-*maximal order in any of the fields in Tables 1 and 2 below.*

Pınar Kılıçer recently proved that all cyclic quartic CM-fields K with $S_{\mathcal{O}_K} = I_{K^r}$ appear in Tables 1 and 2. Together with that result, which which will appear in her PhD thesis, Theorem 13 leads to the following.

Theorem 14 (B.-Kılıçer-S.)**.** *The* 21 *curves of Theorems 12 and 13 are (up to $\overline{\mathbb{Q}}$-isomorphism) exactly the curves $C/\mathbb{Q}$ of genus two such that* $\mathrm{End}(J(C)_{\overline{\mathbb{Q}}})\otimes\mathbb{Q}$ *is a quartic field.*

Finally, we computed the Igusa invariants of D numerically with high precision, leading to the following.

Conjecture 15. *The curve D is isomorphic over $\overline{\mathbb{Q}}$ to*

$$D' : y^2 = 4x^5 + 40x^4 - 40x^3 + 20x^2 + 20x + 3.$$

The curve C was found before by David Kohel, while the curve D' is new. Its absolute Igusa invariants are equal to those of D with high numerical precision.

Theorem 12 is all but proven in [10, 21], and we use our methods to finish the proof in Section 6.1.4. We give the proof of Theorems 13 and 14 in Section 6.1.5.

6.1.2 Background

We start by explaining what in Theorem 12 was already proven, and what remained to be. Murabayashi and Umegaki [10] prove that the 13 fields in Table 1 are the only quartic fields whose maximal orders can be endomorphism rings of genus-two curves over $\mathbb{Q}$. In theory, the algorithm of [17] can compute (with proven correctness) the invariants of all these curves. However, that algorithm is based on denominator bounds that are very far from optimal, so that even the small examples in this list are out of reach.

So we go back to the original publication of the list of curves: van Wamelen [18] computes that each of the 13 fields in this list has 1 or 2 curves corresponding to it, and determines these curves numerically to high precision. This yields his list of 19 curves referenced in the theorem. Van Wamelen [21] later proved that each of his 19 curves does have complex multiplication, and though he does not prove that the endomorphism ring is the *maximal* order, he suggests to prove this by numerically evaluating the absolute Igusa invariants of a large set of period matrices numerically to some small precision, which would finish the proof. We will use our methods to finish the proof that the order is maximal while avoiding numerical computations.

6.1.3 Relation to our results

Denote by $I_{K^r}(f)$ the group of fractional ideals of $\mathcal{O}_{K^r}$ coprime to a fixed integer f. We will first explain how its subgroup $S_{\mathcal{O}}$ relates to Theorems 12 and 13. Let C/k be a curve of genus two over a number field, and suppose that the endomorphism ring $\mathrm{End}(J(C)_{\overline{k}})$ is isomorphic to an order $\mathcal{O}$ in a quartic field K.

Then K is a CM-field, and the theory of complex multiplication gives us some CM-type belonging to the isomorphism $\iota : \mathcal{O} \to \mathrm{End}(J(C)_{\overline{k}})$. Let (K^r, Φ^r) be the reflex of (K, Φ). By the Main Theorem of Complex Multiplication for arbitrary orders [12, §17.3, Main Theorem 3], the composite $k \cdot K^r$ contains the unramified class field k_1 of K^r corresponding to the ideal group $S_{\mathcal{O}} \subset I_{K^r}(f)$.

In particular, if $k = \mathbb{Q}$, then $k_1 = K^r$, so the inclusions $S_{\mathcal{O}} \subset S_{\mathcal{O}_K} \subset I_{K^r}(f)$ are equalities. The following result explicitly generates a minimal order with this property.

Lemma 16. *Let $K \ncong \mathbb{Q}(\zeta_5)$ be a non-biquadratic quartic CM-field with $S_{\mathcal{O}_K} = I_{K^r}$. Let the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset \mathcal{O}_{K^r}$ be generators of the ray class group of K^r modulo f, and let $\mu_i \in K^\times$ be generators of $N_{\Phi^r}(\mathfrak{a}_i)$ such that $\mu_i\overline{\mu_i} \in \mathbb{Q}$.*

Let $\mathcal{O}$ be an order in K such that $f\mathcal{O}_K \subset \mathcal{O}$. We have $S_{\mathcal{O}} = I_{K^r}$ if and only if $\mathcal{O} \supset \mathcal{O}_{min,f} := \mathbb{Z}[\mu_i : i \in \{1, \ldots, n\}] + f\mathcal{O}_K$.

Proof. The $\mu_i \in \mathcal{O}_K$ exist as $S_{\mathcal{O}_K} = I_{K^r}$, and they are uniquely determined up to roots of unity, hence uniquely determined up to sign as $K \ncong \mathbb{Q}(\zeta_5)$. Since $\mathcal{O}$ is a ring and $S_{\mathcal{O}} = I_{K^r}$, both μ_i and $-\mu_i$ are in $\mathcal{O}$ for each i, hence $\mathcal{O}$ contains $\mathcal{O}_{\min,f}$. Conversely, if $\mathcal{O}$ contains $\mathcal{O}_{\min,f}$, then $S_{\mathcal{O}} = I_{K^r}$. □

6.1.4 The case of maximal orders (proof of Theorem 12)

The first curve $y^2 = x^5 + 1$ is well-known to have endomorphism ring $\mathbb{Z}[\zeta_5]$ [12, Example 15.4.2], and van Wamelen computed (as mentioned above) that it is unique with this property.

Next, [21], or more precisely, its data set [20], gives, for each of the other 12 fields in Table 1, an order $\mathcal{O}'$ with a proof that $\mathcal{O} := \mathrm{End}(J(C)_{\overline{\mathbb{Q}}}) \supset \mathcal{O}'$ holds for the curve(s) corresponding to that field. We give these orders in Table 1. As $J(C)$ is principally polarised, the Rosati involution maps $\mathcal{O}$ into itself, and since the Rosati involution acts as complex conjugation on $K = \mathbb{Q}(\mathcal{O})$, this implies $\mathcal{O} \supset \mathcal{O}' + \overline{\mathcal{O}'} =: \mathcal{O}''$. At the same time, as K has no imaginary quadratic subfields, the endomorphism ring $\mathcal{O}$ is an order in K by [9, Theorem 1.3.3].

Next, we take f such that $f\mathcal{O}_K \subset \mathcal{O}''$ and compute $\mathcal{O}_{\min,f}$ as in Lemma 16 using Sage [13]. That lemma then gives $\mathcal{O} \supset \mathcal{O}'' + \mathcal{O}_{\min,f} =: \mathcal{O}'''$, so we compute the latter ring. Note that this ring does not depend on the CM-type Φ appearing in Lemma 16. Indeed, the reflex field $K^r \subset \mathbb{C}$ is the unique subfield isomorphic to K, and as $\mathrm{Gal}(K^r/\mathbb{Q}) \cong C_4$, all CM-types of K^r with values in K are of the form $\Phi^r \circ \sigma$ with $\sigma \in \mathrm{Gal}(K^r/\mathbb{Q})$, so $N_{\Phi^r\circ\sigma}(\mathfrak{a}_i) = N_{\Phi^r}(\sigma(\mathfrak{a}_i))$.

The resulting orders $\mathcal{O}'''$ are equal to $\mathcal{O}_K$ in all but two cases. In the other two, we use Sage [13] to compute the principally polarised ideal classes of $\mathcal{O}'''$ as in [7, Section 4.3], and find that each of them has CM by the maximal order. This proves Theorem 12. □

$[D, A, B]$	n	χ	i_1	i_2	i_3
$[5, 5, 5]$	1				
$[8, 4, 2]$	1	$x^4 + 4x^2 + 2$	1	1	1
$[13, 13, 13]$	1	$x^4 - x^3 + 2x^2 + 4x + 3$	3	1	1
$[5, 10, 20]$	2	$x^4 + 10x^2 + 20$	4	4	2
$[5, 65, 845]$	2	$x^4 - x^3 + 16x^2 - 16x + 61$	19	1	1
$[29, 29, 29]$	1	$x^4 - x^3 + 4x^2 - 20x + 23$	7	1	1
$[5, 85, 1445]$	2	$x^4 - x^3 + 21x^2 - 21x + 101$	29	1	1
$[37, 37, 333]$	1	$x^4 - x^3 + 5x^2 - 7x + 49$	21	3	1
$[8, 20, 50]$	2	$x^4 + 20x^2 + 50$	25	25	1
$[13, 65, 325]$	2	$x^4 - x^3 + 15x^2 + 17x + 29$	23	1	1
$[13, 26, 52]$	2	$x^4 + 26x^2 + 52$	36	36	2
$[53, 53, 53]$	1	$x^4 - x^3 + 7x^2 + 43x + 47$	13	1	1
$[61, 61, 549]$	1	$x^4 - x^3 + 8x^2 - 42x + 117$	39	3	1

Table 1: In Section 6.1.4, we define orders $\mathcal{O}', \mathcal{O}'', \mathcal{O}'''$ of indices i_1, i_2, i_3 in their normal closures as follows. Let $\mathcal{O}' := \mathbb{Z}[x]/(\chi)$, then its field of fractions K is isomorphic to $\mathbb{Q}[X]/(X^4 + AX^2 + B)$ and contains the real quadratic field of discriminant D. Van Wamelen proves that his n curves corresponding to K have endomorphism ring containing $\mathcal{O}'$. We prove that this implies that the endomorphism ring contains $\mathcal{O}'' = \mathcal{O}' + \overline{\mathcal{O}'}$ and $\mathcal{O}''' = \mathcal{O}'' + \mathcal{O}_{\min, i_2}$.

6.1.5 The case of non-maximal orders

Next, we explain how our results and some additional computations prove Theorem 13. Details of the computations will become available online as a Sage [13] file, and we give the main steps and ideas here. Let $C/\mathbb{Q}$ satisfy $\mathcal{O} \cong \mathrm{End}(J(C)_{\overline{\mathbb{Q}}})$ for some order $\mathcal{O}$ in some quartic number field K. Then as in Section 6.1.3, we have $S_{\mathcal{O}_K} = I_{K^r}$. We took all cyclic quartic CM-fields with this property from Bouyer-Streng [6], which is conjectured to be complete. This is a set of of 20 fields, listed in Tables 1 and 2 (see also [6]). We also independently enumerated all quartic CM-fields with discriminant below some bound and found the same list of fields, so we conjectured that this list is complete.

For each of the $20 - 1 = 19$ fields $K \ncong \mathbb{Q}(\zeta_5)$, we did the following computations. For each prime $p \mid 2 \cdot 3 \cdot N_{K_0/\mathbb{Q}}(\mathrm{disc}(K/K_0))$, we use Sage [13] to compute

$[D, A, B]$
$[5, 15, 45]$
$[5, 30, 180]$
$[5, 35, 245]$
$[5, 105, 2205]$
$[8, 12, 18]$
$[17, 119, 3332]$
$[17, 255, 15300]$

Table 2: The known fields with $S_{\mathcal{O}_K} = I_{K^r}$ that are not in Table 1, given by triples $[D, A, B]$ with $K = \mathbb{Q}[X]/(X^4 + AX^2 + B)$ and $\mathrm{disc}(K_0) = D$.

the sequence of rings $A_k = \mathcal{O}_{\min,p^k}$ for $k = 0, 1, \ldots$ until it stabilizes, which we recognize as follows.

Lemma 17. *If $A_{k+1} = A_k$, then for all $l \geq k$, we have $A_l = A_k$.*

Proof. Let $A = A_{k+2}$. It suffices to prove $A = A_{k+1}$. Note that for $n \leq k+2$, we have $A_n = A + p^n\mathcal{O}_K$. In particular, we have $A \subset A_{k+1} = A + p^k\mathcal{O}_K$, where the quotient for the inclusion is a power of $(\mathbb{Z}/p\mathbb{Z})$. Therefore, multiplying on the right with p reverses the inclusion, so $A \supset pA + p^{k+1}\mathcal{O}_K$, so $A \supset A + p^{k+1}\mathcal{O}_K$, which is what we needed to show. □

For our list of 19 fields, it turns out that the chain always stabilises at $p^k = 1$, except in the case $p = 2$ for 7 of the fields, where it stabilises at 2^1 with $[\mathcal{O}_K : \mathcal{O}_{\min,2}] \in \{2, 4\}$. In particular, as no odd prime power greater than one appears, we have $\mathcal{O}_{\min,f} = \mathcal{O}_{\min,2^k}$ for $k \in \{0, 1\}$ for all our 19 fields K. For the 7 fields with $k = 1$, we compute all non-maximal superorders of $\mathcal{O}_{\min,2}$ and their principally polarised ideal classes using Sage. We can check the existence of $(2, 2)$-isogenies in a proven manner on the level of these principally polarised ideal classes, as the polarised complex tori corresponding to $(\mathfrak{a}_1, \xi_1)$ and $(\mathfrak{a}_2, \xi_2)$ are (ℓ, ℓ)-isogenous if and only if there exists $\mu \in K^\times$ with $\mathfrak{a}_1 \subset \mu^{-1}\mathfrak{a}_2$ and $\xi_1 = \ell\mu\overline{\mu}\xi_2$. The computations above yield the following result.

Lemma 18. *Each principally polarised ideal class with multiplicator ring a non-maximal order $\mathcal{O}$ with $S_\mathcal{O} = I_{K^r}$ in one of our 19 fields $K \ncong \mathbb{Q}(\zeta_5)$ is $(2, 2)$-isogenous to a unique principally polarised ideal class of the maximal order of K.* □

This proves Theorem 13 for the fields in Table 2: as the (unique $(2, 2)$-isogenous) curves with CM by the maximal order are not stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, neither are the curves with CM by the non-maximal orders.

For the $13 - 1 = 12$ fields $K \ncong \mathbb{Q}(\zeta_5)$ in Table 1, we used the AVIsogenies [3] Magma [5] package to compute all principally polarised abelian surfaces over $\mathbb{Q}$ that are $(2, 2)$-isogenous to those of Theorem 12. This yielded no curves not covered by Theorem 12, hence proves Theorem 13 outside of the case $K = \mathbb{Q}(\zeta_5)$.

This leaves the field $K = \mathbb{Q}(\zeta_5)$, where Lemma 16 does not directly apply. There we do have $\mathcal{O} \supset \mathbb{Z}[\zeta_5^{e_i}\mu_i : i] + f\mathcal{O}_K$ with $0 \leq e_i < 5$, so the computations are still finite, but a little more complicated. In the end, this yields 7 orders, the indices of which all happen to be prime powers (of 2, 3, or 5 to be precise). We compute the corresponding period matrices, and they all turn out to be related to $y^2 = x^5 + 1$ by a $(3, 3)$-isogeny, a $(5, 5)$-isogeny, or a chain of at most two $(2, 2)$-isogenies.

In the case of the $(5, 5)$-isogeny, we found a unique period matrix, corresponding to some curve D, and its invariants are equal to those of D' to high precision. For the $(3, 3)$-isogeny, we find using AVIsogenies that over $\overline{\mathbb{F}_{23}}$, there are 40 curves that are $(3, 3)$-isogenous to $F : y^2 = x^5 + 1$, none of which have their moduli in $\mathbb{F}_{23}$. As these are the reductions of the 40 curves over $\overline{\mathbb{Q}}$ that are $(3, 3)$-isogenous to F, we find that none of them are defined over $\mathbb{Q}$.

For the $(2, 2)$-isogenies, we used the Richelot isogeny code of AVIsogenies directly over $\mathbb{Q}$. It returned the curve C from Theorem 13, which is $(2, 2)$-isogenous to F, and no other curve over $\mathbb{Q}$ that is $(2, 2)$-isogenous to C or F. This shows that F has CM by a non-maximal order $\mathcal{O} \supset 1 + 2\mathcal{O}_K$. The only such order with $S_\mathcal{O} = I_{K^r}$ for which period matrices exist is the one given in

Theorem 13. A Sage computation with principally polarised ideal classes shows that every curve with CM by an order $\mathcal{O}$ with $S_{\mathcal{O}} = I_{K^r}$ and even index in $\mathcal{O}_K$ is $(2,2)$-isogenous to C or F, and we check using AVIsogenies that no such curve exists other than C and F themselves; this proves Theorem 13 for the one remaining field $\mathbb{Q}(\zeta_5)$. Theorem 14 will follow from compleness of Table 2, which is part of Kılıçer's PhD thesis. □

To prove $D \cong D'$, it would suffice to show that D' has complex multiplication over $\overline{\mathbb{Q}}$ by an order in $\mathbb{Q}(\zeta_5)$, which can be done using the methods of [21], or by showing that it is isogenous over $\overline{\mathbb{Q}}$ to $F : y^2 = x^5 + 1$.

6.2 Computation of endomorphism rings

Let $\mathcal{A}$ be an ordinary principally polarised abelian surface defined over a finite field k of cardinality q. The characteristic polynomial of its Frobenius endomorphism π may be computed in polynomial time in $\log(q)$ [11]; this gives the CM-field $K = \mathbb{Q}(\pi)$ of which the endomorphism ring of $\mathcal{A}$ is an order $\mathrm{End}(\mathcal{A})$ containing $\mathbb{Z}[\pi, \overline{\pi}]$ and stable under complex multiplication [22].

Recently, the first-named author generalised to abelian varieties [2] a method to compute this order in subexponential time for elliptic curves [4, 1]. Its main idea is to exploit complex multiplication theory to determine the structure of the polarised class group $\mathfrak{C}(\mathrm{End}(\mathcal{A}))$ by evaluating isogenies from the abelian variety $\mathcal{A}$; then, the endomorphism ring $\mathrm{End}(\mathcal{A})$ may be identified amongst orders $\mathcal{O}$ satisfying $\mathfrak{C}(\mathcal{O}) = \mathfrak{C}(\mathrm{End}(\mathcal{A}))$ by computing it locally at primes which divide the index between two such orders.

Fix $f = [\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ and restrict to ideals coprime to f for the remainder of this section, so that the groups $P_{\mathcal{O}} \subset I_{\mathcal{O}} \subset I_{\mathcal{O}_K}$ may be compared as $\mathcal{O}$ ranges through candidate endomorphism rings. For efficiency reasons, rather than computing $\mathfrak{C}(\mathcal{O}) = I_{\mathcal{O}}/P_{\mathcal{O}}$ by finding sufficiently many elements of $P_{\mathcal{O}}$, this algorithm fixes an arbitrary CM-type Φ of K and only uses elements of $\mathrm{N}_{\Phi^r}(\mathrm{N}_{\Phi}(p_{\mathcal{O}}))$, where $p_{\mathcal{O}}$ stands for the group of principal ideals of $\mathcal{O}$. For a given order $\mathcal{O}$, determining whether elements of $\mathrm{N}_{\Phi^r}(\mathrm{N}_{\Phi}(p_{\mathcal{O}}))$ are trivial in $\mathfrak{C}(\mathrm{End}(\mathcal{A}))$ can be done in subexponential time in $\log(q)$. Then, the algorithm incurs a polynomial cost in $v_\ell = \ell^{\mathrm{val}_\ell(f)}$ to compute the endomorphism ring locally at ℓ using [8] for each prime factor ℓ of

$$\mathrm{lcm}\left\{ [\mathcal{O} + \mathcal{O}' : \mathcal{O} \cap \mathcal{O}'] : \begin{array}{l} \mathrm{N}_{\Phi}(p_{\mathcal{O}}) \subset S_{\mathcal{O}'} \\ \mathrm{N}_{\Phi}(p_{\mathcal{O}'}) \subset S_{\mathcal{O}} \end{array} \right\}, \tag{7}$$

where $\mathcal{O}$ and $\mathcal{O}'$ range through all orders of K containing $\mathbb{Z}[\pi, \overline{\pi}]$ stable under complex conjugation, and the map N_{Φ} takes an ideal of $p_{\mathcal{O}}$ (resp. $p_{\mathcal{O}'}$) to I_{K^r}. The results of the preceding sections would apply directly to this algorithm if (7) had $\mathrm{N}_{\Phi}(p_{\mathcal{O}})$ replaced by $S_{\mathcal{O}}$ and $\mathrm{N}_{\Phi}(p_{\mathcal{O}'})$ by $S_{\mathcal{O}'}$; nevertheless, those two groups are closely related as the following lemma shows.

Lemma 19. *For any order $\mathcal{O}$ we have $(S_{\mathcal{O}} \cap \mathrm{N}_{\Phi}(I_{\mathcal{O}}))^2 \subset \mathrm{N}_{\Phi}(p_{\mathcal{O}}) \subset S_{\mathcal{O}}$.*

Proof. Consider the composition $I_K \xrightarrow{\mathrm{N}_{\Phi}} I_{K^r} \xrightarrow{\mathrm{N}_{\Phi^r}} I_{\mathcal{O}_K}$ where I_K and I_{K^r} are the groups of invertible fractional ideals in $\mathcal{O}_K$ and $\mathcal{O}_{K^r}$ respectively, and recall from the proof of Lemma 4 that $\mathrm{N}_{\Phi^r}\mathrm{N}_{\Phi}(\mathfrak{a}) = \mathfrak{a}^2(\mathfrak{a}\overline{\mathfrak{a}})^{\sigma}$; if $\mathfrak{a}$ admits a generator coprime to f in $\mathcal{O}$, its image through $\mathrm{N}_{\Phi^r} \circ \mathrm{N}_{\Phi}$ thus also does. Therefore the type norm maps $p_{\mathcal{O}}$ to a subset of $S_{\mathcal{O}}$.

Let $\mathfrak{b}$ lie in the intersection of $S_{\mathcal{O}}$ and $\mathrm{N}_\Phi(I_{\mathcal{O}})$. This means that, for some $(\mathfrak{a},\alpha)\in I_{\mathcal{O}}$, we have $\mathfrak{b}=\mathrm{N}_\Phi(\mathfrak{a},\alpha):=\mathrm{N}_\Phi(\mathfrak{a})$ and $\mathrm{N}_{\Phi^r}\mathrm{N}_\Phi(\mathfrak{a})\in P_{\mathcal{O}}$. Equation (2) then states that $(\mathfrak{a},\alpha)^2$ belongs to $P_{\mathcal{O}}$; by composing with N_Φ, we find that $\mathfrak{b}^2$ belongs to $\mathrm{N}_\Phi(P_{\mathcal{O}})$, and hence to $\mathrm{N}_\Phi(p_{\mathcal{O}})$. □

Therefore $\mathrm{N}_\Phi(p_{\mathcal{O}})$ is not much different from $S_{\mathcal{O}}$; in fact, similarly to Theorem 3 we have:

Corollary 20. *Let $\mathcal{O}$ and $\mathcal{O}'$ be two orders satisfying the conditions of (7). The indices $[\mathcal{O}:\mathcal{O}^\circ]$ and $[\mathcal{O}_0:\mathcal{O}_0^\circ]$ have the same valuation at all primes $\ell>41$, and even $\ell>7$ when $\mathcal{O}\neq\mathbb{Z}[\zeta_5]$.*

Proof. By the above lemma, the conditions of (7) imply $(S_{\mathcal{O}}\cap\mathrm{N}_\Phi(I_{\mathcal{O}}))^2\subset S_{\mathcal{O}'}$; as in Section 3 we thus have

$$\ker(\mathfrak{C}(\mathcal{O}^\circ)\to\mathfrak{C}(\mathcal{O}))^4\subset\ker(\mathfrak{C}(\mathcal{O}^\circ)\to\mathfrak{C}(\mathcal{O}')).$$

Indeed, let $(\mathfrak{a},\alpha)^4$ be a representative of an element in the first kernel; $(\mathfrak{a},\alpha)^4=\mathrm{N}_{\Phi^r}\mathrm{N}_\Phi(\mathfrak{a})^2$ holds in $\mathfrak{C}(\mathcal{O}^\circ)$ by (2) and we have $\mathrm{N}_\Phi(\mathfrak{a})^2\in(S_{\mathcal{O}}\cap\mathrm{N}_\Phi(I_{\mathcal{O}}))^2$ by assumption. In particular, we have $\mathrm{N}_{\Phi^r}\mathrm{N}_\Phi(\mathfrak{a})^2\in\mathrm{N}_{\Phi^r}(S_{\mathcal{O}'})$, so the class of $(\mathfrak{a},\alpha)^4$ in $\mathfrak{C}(\mathcal{O}^\circ)$ becomes trivial in $\mathfrak{C}(\mathcal{O}')$.

Now, using the same proof as for Proposition 6 (albeit replacing two by four in all exponents), we deduce that for any two orders $\mathcal{O},\mathcal{O}'$ satisfying the conditions of (7) the kernel (5) is of exponent at most four. The proof of Proposition 8 then carries through for all primes $p>41$ in the case where $\mathcal{O}\neq\mathbb{Z}[\zeta_5]$, and $p>7$ for all other orders. □

As a consequence, we now establish that the sum $\sum_\ell v_\ell$ where ℓ ranges through prime factors of (7) is almost always small, which implies that the algorithm of [2] is of subexponential complexity.

Proposition 21. *Let $(\mathcal{A}_i/\mathbb{F}_{q_i})_{i\in\mathbb{N}}$ be a sequence of ordinary abelian varieties defined over fields of monotonously increasing cardinality $q_i\to\infty$. Denote by $v_i=[\mathcal{O}_{\mathbb{Q}(\pi_i)}:\mathbb{Z}[\pi_i,\overline{\pi}_i]]$ their conductor gaps, by $n_i=\mathrm{N}_{K_0/\mathbb{Q}}(\mathrm{disc}(K/K_0))$ the norm of the relative discriminant of their CM-fields $K=\mathbb{Q}(\pi_i)$. Assume that there exists a constant C such that, for all positive integers u and m:*

- *the proportion of indices $i<m$ for which $u|v_i$ is at most C/u;*
- *the proportion of indices $i<m$ for which $u|v_i$ and $u|n_i$ is at most C/u^2.*

Then, for any $\tau>0$, all prime factors ℓ of (7) are such that $v_{i,\ell}=\ell^{\mathrm{val}_\ell v_i}$ is smaller than $L(q_i)^\tau$, except for a zero-density subset of indices $i\in\mathbb{N}$, where $L(x)=\exp\sqrt{\log x\cdot\log\log x}$.

Proof. Fix an index i and let ℓ be a prime factor of v_i. If ℓ^2 does not divide v_i, then, locally at ℓ, out of two distinct orders containing $\mathbb{Z}[\pi_i,\overline{\pi}_i]$, one must be maximal; by the proof of Theorem 2, the quantity (7) thus has no ℓ-part unless $\ell\leq 41$ or $\ell|n_i$. As a consequence, for any fixed integer $M\geq 41$, all pairs of indices $i<m$ and primes ℓ dividing (7) such that $v_{i,\ell}>L(q_i)^\tau$ satisfy at least one of the following conditions:

- the index i satisfies $L(q_i)^\tau\leq M$;

- $\mathrm{val}_\ell\, v_i = 1$ and $\ell > M$ divides $\gcd(v_i, n_i)$;
- $\mathrm{val}_\ell\, v_i > 1$ and $v_{i,\ell} > M$ divides v_i.

Since $v_i < 64q_i^2$ [2, Lemma 3.2] we have $v_{i,\ell} < 64q_m^2$ for all primes ℓ and indices $i < m$, thanks to the monotony of q_i. Hence the proportion of indices $i < m$ for which (7) admits a prime factor ℓ such that $v_{i,\ell} > L(q_i)^\tau$ is bounded by

$$\frac{\#\{i : L(q_i)^\tau \leq M\}}{m} + \sum_{M<\ell<64q_m^2} \frac{C}{\ell^2} + \sum_{2\leq\alpha\leq 6+2\log_2 q_m} \left(\sum_{M^{1/\alpha}<\ell\leq M^{1/(\alpha-1)}} \frac{C}{\ell^\alpha} \right)$$

where each term corresponds to one of the above conditions, and the variable α represents $\mathrm{val}_\ell\, v_i$. Note that the bound $\ell \leq M^{1/(\alpha-1)}$ in the last sum is here to prevent counting the same prime ℓ for multiple values of α.

By bounding each sum, we further deduce that the density of such indices is less than

$$\lim_{m\to\infty} \left(\frac{\#\{i : L(q_i)^\tau < M\}}{m} + \frac{C}{M} + \sum_{\alpha>1} \frac{C}{\alpha-1} \left(\frac{1}{M^{\frac{\alpha-1}{\alpha}}} - \frac{1}{M} \right) \right)$$

For M large enough, the second and third terms can be made arbitrarily small; then, the first term vanishes as m goes to infinity; the density is therefore zero. □

Note that the conditions require that the integers v_i present certain divisibility properties of integers drawn uniformly at random (say, from $\{1, \ldots, 64q_i^2\}$) and independently from the n_i. They are experimentally observed to hold for the two main families which are of interest to this work, namely random isomorphism classes of abelian varieties, and random isomorphism classes of abelian varieties with complex multiplication by a prescribed field, defined over finite fields of increasing cardinality. See [2] for details.

Acknowledgements

The authors would like to thank David Gruenewald for helpful discussions. The first-named author wishes to thank the Mathematics Research Centre of the University of Warwick for their hospitality while most of this work was done.

References

[1] Gaetan Bisson. Computing endomorphism rings of elliptic curves under the GRH. *Journal of Mathematical Cryptology.*, 5(2):101–113, 2011.

[2] Gaetan Bisson. Computing endomorphism rings of abelian varieties. `http://arxiv.org/abs/1209.1189`, 2012.

[3] Gaetan Bisson, Romain Cosset, and Damien Robert. *AVIsogenies, a library for computing isogenies between abelian varieties*, 2010. `http://avisogenies.gforge.inria.fr/`.

[4] Gaetan Bisson and Andrew V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *Journal of Number Theory*, 131(5):815–831, 2011.

[5] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system: the user language. *Journal of Symbolic Computation*, 24(3–4):235–265, 1997.

[6] Florian Bouyer and Marco Streng. Examples of CM curves of genus two defined over the reflex field. To appear, 2012.

[7] Reinier Bröker, Kristin Lauter, and Marco Streng. Abelian surfaces admitting an (l, l)-endomorphism. `http://arxiv.org/abs/1106.1884`, 2011.

[8] Kirsten Eisenträger and Kristin E. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. In François Rodier and Serge Vladut, editors, *Arithmetic, Geometry and Coding Theory — AGCT 2010*, volume 21 of *Séminaires et Congrès*, pages 161–176. Société Mathématique de France, 2009.

[9] Serge Lang. *Complex Multiplication*, volume 255 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1983.

[10] Naoki Murabayashia and Atsuki Umegaki. Determination of all $\mathbb{Q}$-rational CM-points in the moduli space of principally polarized abelian surfaces. *Journal of Algebra*, 235(1):267–274, 2001.

[11] Jonathan Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Mathematics of Computation*, 55(192):745–763, 1990.

[12] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, 1961.

[13] William A. Stein et al. *Sage Mathematics Software (Version 5.2)*. The Sage Development Team, 2012. `http://www.sagemath.org/`.

[14] Peter Stevenhagen. *The arithmetic of number rings*, volume 44 of *Mathematical Sciences Research Institute Publications*, pages 209–266. Cambridge University Press, 2008.

[15] Marco Streng. *Complex multiplication of abelian surfaces*. PhD thesis, Universiteit Leiden, 2010. `http://www.math.leidenuniv.nl/~streng/thesis.pdf`.

[16] Marco Streng. An explicit reciprocity law for Siegel modular functions. `http://arxiv.org/abs/1201.0020`, 2011.

[17] Marco Streng. Computing Igusa class polynomials. To appear in Mathematics of Computation, 2012.

[18] Paul van Wamelen. Equations for the Jacobian of a hyperelliptic curve. *Transactions of the American Mathematical Society*, 350(8):3083–3106, 1998.

[19] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Mathematics of Computation*, 68(225):307–320, 1999.

[20] Paul van Wamelen. Genus 2 CM curves defined over the rationals. `https://www.math.lsu.edu/~wamelen/CMcurves.txt`, 1999.

[21] Paul van Wamelen. Proving that a genus 2 curve has complex multiplication. *Mathematics of Computation*, 68(228):1663–1677, 1999.

[22] William C. Waterhouse. Abelian varieties over finite fields. *Annales Scientifiques de l'École Normale Supérieure*, 2(4):521–560, 1969.